Amendments to the Claims

Claim 1 (currently amended): A computer program product for using biometrics on pervasive devices for mobile identification, said computer program product embodied on a medium readable by said pervasive device and comprising:

programmable code means for capturing, using a biometric input reader which is attached to or incorporated within a mobile pervasive device possessed by a ~~first party~~ user, biometric data of ~~a second party~~ another being encountered by said possessor; and

programmable code means for identifying said encountered being ~~second party~~ using said captured biometric data by comparing said captured biometric data to previously-stored biometric data.

Claim 2 (original): The computer program product according to Claim 1, further comprising:

programmable code means for transmitting said captured biometric data from said mobile pervasive device to a remote server;

programmable code means for retrieving, by said remote server, information from a repository using said transmitted biometric data; and

programmable code means for returning said retrieved information to said mobile pervasive device.

Claim 3 (original): The computer program product according to Claim 2, wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds.

Claim 4 (original): The computer program product according to Claim 2, wherein said retrieved information comprises access rights of a party to whom said biometric data corresponds.

Claim 5 (original): The computer program product according to Claim 2, wherein said retrieved information comprises protected information not locally accessible to said mobile pervasive device.

Claim 6 (currently amended): The computer program product according to Claim 2 or Claim 5, further comprising:

programmable code means for filtering, by said remote server, said retrieved information based upon a determined identity of said ~~second party~~ encountered being; and

wherein said returned retrieved information is said filtered retrieved information.

Claim 7 (original): The computer program product according to Claim 1, wherein said mobile pervasive device further comprises a locally-stored repository containing said previously-stored biometric data, and wherein said programmable code means for identifying compares, by said mobile pervasive device, said captured biometric data to said previously-stored biometric data in said locally-stored repository.

Claim 8 (original): The computer program product according to Claim 1, wherein said computer program product is used to enable on-demand creation of a secure meeting site by repeating operation of said programmable code means for capturing and said programmable code means for identifying for each of a plurality of meeting attendees.

Claim 9 (currently amended): The computer program product according to Claim 1, wherein said computer program product is used to exchange a trusted message by performing operation of said programmable code means for capturing and said programmable code means for identifying wherein said ~~second party~~ encountered being is a potential recipient of said trusted message.

Claim 10 (currently amended): A system for using biometrics on pervasive devices for mobile identification, said system comprising:

a mobile pervasive device possessed by ~~a first party~~ user;

a biometric input reader attached to or incorporated within said mobile pervasive device;

means for capturing biometric data of ~~a second party~~ another being encountered by said possessor, using said biometric input reader; and

means for identifying said ~~second party~~ encountered being using said captured biometric data by comparing said captured biometric data to previously-stored biometric data.

Claim 11 (original): The system according to Claim 10, further comprising:

means for transmitting said captured biometric data from said mobile pervasive device to a remote server;

means for retrieving, by said remote server, information from a repository using said transmitted biometric data; and

means for returning said retrieved information to said mobile pervasive device.

Claim 12 (original): The system according to Claim 11, wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds.

Claim 13 (original): The system according to Claim 11, wherein said retrieved information comprises access rights of a party to whom said biometric data corresponds.

Claim 14 (original): The system according to Claim 11, wherein said retrieved information comprises protected information not locally accessible to said mobile pervasive device.

Claim 15 (currently amended): The system according to Claim 11 or Claim 14, further comprising:

means for filtering, by said remote server, said retrieved information based upon a determined identity of said ~~second party~~ encountered being; and

wherein said returned retrieved information is said filtered retrieved information.

Claim 16 (original): The system according to Claim 10, wherein said mobile pervasive device further comprises a locally-stored repository containing said previously-stored biometric data, and wherein said means for identifying compares, by said mobile pervasive device, said captured biometric data to said previously-stored biometric data in said locally-stored repository.

Claim 17 (original): The system according to Claim 10, wherein said system is used to enable on-demand creation of a secure meeting site by repeating operation of said means for capturing and said means for identifying for each of a plurality of meeting attendees.

Claim 18 (currently amended): The system according to Claim 10, wherein said system is used to exchange a trusted message by performing operation of said means for capturing and said means for identifying wherein said~~ second party~~ encountered being is a potential recipient of said trusted message.

Claim 19 (currently amended): A method for using biometrics on pervasive devices for mobile identification, said method comprising the steps of:

capturing, using a biometric input reader attached to or incorporated within a mobile pervasive device possessed by ~~a first party~~ user, biometric data of~~ a second party~~ another being encountered by said possessor; and

identifying said~~ second party~~ encountered being using said captured biometric data by comparing said captured biometric data to previously-stored biometric data.

Claim 20 (original): The method according to Claim 19, further comprising the steps of:

transmitting said captured biometric data from said mobile pervasive device to a remote server;

retrieving, by said remote server, information from a repository using said transmitted biometric data; and

returning said retrieved information to said mobile pervasive device.

Claim 21 (original): The method according to Claim 20, wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds.

Claim 22 (original): The method according to Claim 20, wherein said retrieved information comprises access rights of a party to whom said biometric data corresponds.

Claim 23 (original): The method according to Claim 20, wherein said retrieved information comprises protected information not locally accessible to said mobile pervasive device.

Claim 24 (currently amended): The method according to Claim 20 or Claim 23, further comprising the step of:

filtering, by said remote server, said retrieved information based upon a determined identity of said ~~second party~~ encountered being; and

wherein said returned retrieved information is said filtered retrieved information.

Claim 25 (original): The method according to Claim 19, wherein said mobile pervasive device further comprises a locally-stored repository containing said previously-stored biometric data, and wherein said identifying step compares, by said mobile pervasive device, said captured biometric data to said previously-stored biometric data in said locally-stored repository.

Claim 26 (original): The method according to Claim 19, wherein said method is used to enable on-demand creation of a secure meeting site by repeating operation of said capturing step and said identifying step for each of a plurality of meeting attendees.

Claim 27 (currently amended): The method according to Claim 19, wherein said method is used to exchange a trusted message by performing operation of said capturing step and said identifying step wherein said ~~second party~~ encountered being is a potential recipient of said trusted message.